

# United States District Court

for the  
Western District of New York

## In the Matter of the Search of

*(Briefly describe the property to be searched or identify the person by name and address.)*

The following accounts maintained, controlled, or operated by Rackspace US, Inc.:

polytainersinc.company.com;  
bsattaur@polytainersinc.company.com;  
mjennings@polytainersinc.company.com;  
sachdeva@polytainersinc.company.com;  
kowalewski@polytainersinc.company.com;  
jennings@polytainersinc.company.com

Case No. 18-mj-1176

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: See Attachment A

located in the Western District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:  
See Attachment B.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of Title 18 U.S.C. § 1343 and/or Title 18 U.S.C. §§ 1030(a)(4) and/or 1030(a)(5)(C) *[statutory violation(s)]*.

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


  
Applicant's signature

DOUGLAS J. MILLER  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION  
Printed name and title

Sworn to before me and signed in my presence.

Date: October 19, 2018

City and state: Buffalo, New York

  
Judge's signature

HONORABLE JEREMIAH J. MCCARTHY  
UNITED STATES MAGISTRATE JUDGE  
Printed name and Title

**AFFIDAVIT IN SUPPORT OF**  
**APPLICATION FOR SEARCH WARRANT**

I, DOUGLAS J. MILLER, being duly sworn, depose and state the following:

**I. INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed for more than twenty two years. I am currently assigned to the Cyber Squad in the Buffalo Division, Buffalo, New York. I have worked cyber investigative matters, that is, matters focused on computer intrusions and cyber related frauds, since May 2017. I have received training in conducting such cyber based investigations, as well as education covering, among other things, hacker techniques and cyber security. Specifically, I have worked or assisted with matters involving unauthorized access to network and email systems, counterintelligence, and counterterrorism. Prior to my employment in the FBI, I received a Master's of Science degree in Accounting and worked as Certified Public Accountant for nine years as an accountant, auditor, consultant, corporate and individual income tax preparer, accounting manager, and controller in private industry. My work in the FBI, as well as the training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. I have also conferred with other FBI Special Agents who have extensive expertise and experience in cyber investigations and digital evidence. The FBI is an agency within the United States Department of Justice, which is a department within the Executive Branch of the United States Government.

2. I make this affidavit in support of an application for a search warrant authorizing the search of the domain **polytainersinc.company.com** and the specified email accounts within that domain: **bsattaur@polytainersinc.company.com**, **mjennings@polytainersinc.company.com**; **sachdeva@polytainersinc.company.com**; **kowalewski@polytainersinc.company.com**; and **jennings@polytainersinc.company.com**. The above domain is registered to Company.com. However, Company.com has subcontracted portions of both the email and domain services for above to Rackspace US, Inc. (hereinafter referred to as "Rackspace") and Weebly, Inc. After speaking with representatives of Company.com and Rackspace, I have determined that all three (3) companies hold evidence related to crimes detailed below. Rackspace, to whom this affidavit is directed, is located at, 1 Fanatical Place, Windcrest, Texas 78218.

3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **Rackspace** to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account, including contents of communications and payment information.

**II. PROBABLE CAUSE THE DOMAIN  
POLYTAINERSINC.COMPANY.COM AND THE SPECIFIED EMAIL  
ACCOUNTS CONTAINED WITHIN THAT DOMAIN, WERE USED TO  
COMMIT FRAUD AND CONTAIN INFORMATION REGARDING THAT  
FRAUD**

4. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations Title 18 U.S.C. 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme) and Title 18 U.S.C. 1030(a)(4) (Fraud and related activity in relation to computers) and/or Title 18 U.S.C. 1030 (a)(5)(C) (Intentional access to a protected computer causing damage or loss) will be found in the domain and email accounts:

**polytainersinc.company.com;  
bsattaur@polytainersinc.company.com;  
mjennings@polytainersinc.company.com;  
sachdeva@polytainersinc.company.com;  
kowalewski@polytainersinc.company.com;  
jennings@polytainersinc.company.com**

5. The information set forth below establishes probable cause that the domain polytainersinc.company.com and the specified email accounts within that domain were utilized in connection with communications used to defraud victim company, Upstate Niagara Cooperative, Inc. (hereinafter referred to as "UNCI"). UNCI is a regional dairy cooperative headquartered in Cheektowaga, New York, producing a range of dairy products for consumers, such as, butter, cottage cheese, cream, ice cream, milk, sour cream, and yogurt. UNCI has primary, New York State based, production facilities in Cheektowaga, NY; New York, NY; Rochester, NY; and West Seneca, NY.

6. From August 28 – 29, 2018, UNCI representatives were in email contact with representatives of their Etobicoke, Ontario, Canada based vendor Polyainers, Inc. Authentic email addresses from Polyainers, Inc. utilize the email schema [first letter of first name][last name]@polyainers.com.

7. On September 4, 2018, several representatives of UNCI received communications from spoofed/impersonator email account **bsattaur@polyainersinc.company.com**. The spoofed/impersonator email purported to originate from legitimate Polyainers, Inc. Accounts Receivable Analyst, Bebe Sattaur, a person with whom UNCI had conducted similar business in the past. Spoofed/impersonator email accounts are created by fraud actors in business email compromise (BEC) scams to appear nearly identical to legitimate email accounts in terms of using a very similar appearing domain and structure schema. In addition, spoofed/impersonator email accounts almost always purport to be from an individual known to have engaged in similar business activity in the past. Note the similarity in appearance between the authentic Polyainers, Inc account of bsattaur@polyainers.com as compared to the address utilized by the fraud actor(s) of **bsattaur@polyainersinc.company.com**.

8. The email from **bsattaur@polyainersinc.company.com** to UNCI included the following text: “Please be aware that payment to our normal business account has been suspended due to high bank charges and all payment by check or wire transfer to our previous business account has been suspended pending when we are able to resolve issues with our account. All payment of due invoice is to be received in our alternative business account.

Kindly acknowledge this email and the alternative account would be forwarded to you for the payment of due invoice.”

9. In many of the communications from **bsattaur@polytainersinc.company.com**, other spoofed email accounts were on the carbon copy (CC) line, including, **mjennings@polytainersinc.company.com**; **sachdeva@polytainersinc.company.com**; **kowalewski@polytainersinc.company.com**; and **jennings@polytainersinc.company.com**.

10. On September 5, 2018, there were multiple email exchanges between the spoofed/impersonator email account **bsattaur@polytainersinc.company.com** and UNCI personnel. The spoofed/impersonator account then sent an email to UNCI representatives, containing the following:

“Kindly note that cutting checks is not acceptable for now, Also find below the information you need for ACH payment.

Bank Name – Wells Fargo

Account Name – Polytainers Inc

Account Number – 8069237918

Routing Number – 051400549

Bank Address – 8118 Sudley Road, Manassas Va 20109”

11. On September 7, 2018, UNCI wire transferred \$212,391.46 to Wells Fargo Bank, using the above instructions. The amount matched actual bills UNCI owed the legitimate company Polytainers, Inc. On September 13, 2018, UNCI initiated a wire transfer,

using the same instructions, for \$354,314.62. The September 13, 2018 wire transfer was returned by Wells Fargo, with a comment stating that the destination account had been identified as fraudulent. The prior amount transferred to UNCI of \$212,391.46 was not returned as it had already been moved out of the account.

12. On September 19, 2018, UNCI received an email from the spoofed/impersonator email account **bsattaur@polytainersinc.company.com** which stated that the next payment would need to go to their Suntrust Bank account, using the following wire transfer instructions, provided via the spoofed/impersonated email account, shortly thereafter:

Account Name – Polytainers Inc.

Account Number – 1000214988908

Routing Number – 061000104

Bank Address – 4601 Jonesboro Road, Union City, GA 30291

13. Follow up investigation determined that on or about June 22, 2018—roughly two months prior to UNCI receiving an e-mail from **bsattaur@polytainers.company.com**—UNCI marketing representative Allison Kowalewski advised her management she, “thought she had done something wrong,” after she had acted on an email received on her company email account, [akowalewski@upstateniagara.com](mailto:akowalewski@upstateniagara.com). UNCI subscribes to Microsoft Office 365 as the platform for their company email service.

14. The suspicious email Kowalewski responded to purported to be from Dropbox.com, a popular file hosting/sharing service, utilized by UNCI, a trusted party.

Kowalewski had attempted to login to her Dropbox.com account, as instructed in the email, using her Microsoft Office 365/company email credentials. However, shortly thereafter, Kowalewski realized she had been tricked into entering her company email user name and password in response to the suspicious/phishing<sup>1</sup> email since her Dropbox.com account login had been set up to utilize her Google login credentials. UNCI changed Kowalewski's password once they learned her company email account login credentials had been compromised, believing incorrectly they had solved all security issues relating to the phishing email.

15. In my training and experience, I have learned that fraud actors running BEC scams will often identify viable targets via online searches. The scammers will then work to obtain the target's email login credentials via phishing. Once target's email login credentials have been harvested, the fraudsters will use the acquired user name/passwords to enter and reconfigure the target's email account to forward emails received, to an email account controlled by the fraudsters. Once achieved, the fraudsters are able to read emails intended for the target. While conducting reconnaissance on a targeted email account, the fraudsters work to identify a point at which they can interject themselves into established communications with spoofed emails, impersonating both legitimate parties. Once done, while both parties continue to communicate via email believing they remain in contact with each other, they are both in reality communicating with the fraudsters. The fraudsters will then continue communications with both parties to the point where payment is required, at

---

<sup>1</sup> Phishing involves the use of emails sent to fraud targets that purport to be sent from a trustworthy source, requesting login credentials for a legitimate purpose.



which time the fraudsters provide “updated”/“new” fund transfer instructions to a victim, to fraudulently obtain any monies remitted.

16. UNCI audited their company email accounts for email forwarding, subsequent to losing the \$212,391.46 to the fraudulent actor(s). They determined Kowalewski’s UNCI email account akowalewski@upstateniagara.com, had been set up to forward emails received to maniar.sam2@gmail.com, an account with no legitimate purpose or connection to UNCI.

### **III. BACKGROUND REGARDING COMPUTER, THE INTERNET, AND EMAIL**

17. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

18. I have had training in the investigation of computer-related crimes. Based on my training, and experience, I know the following:

- a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

- b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and
- c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, than transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

19. Many individual computer users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using cable, telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world.

20. The ISP assigns each user an internet protocol (IP) address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the

same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Thus, by ascertaining the IP address relating to a specific message sent or action taken over the Internet, it is possible to determine the ISP and even the individual computer responsible.

21. The ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, email transaction information, posting information, account application information, IP addresses, and other information both in computer data format and in written record format.

22. A domain is a distinct subset of the internet with addresses sharing a common suffix or under the control of a particular organization or individual. A domain name is formed according to rules and procedures of the domain name system (DNS). The DNS is a decentralized system for computers, services, or other resources connected to the internet or a private network, which translates for addressing purposes, readily memorized domain names, into the IP addresses needed for locating and identifying computer services and devices to which messages are sent or services are requested. The registration of domain names is usually administered by domain name registrars, who sell their services to the public.

#### **IV. BACKGROUND REGARDING RACKSPACE**

23. Based on my training and experience, I have learned the following about Rackspace:

- a. Rackspace is considered an electronic communications service ("ECS") provider because it provides its users access to electronic communications service as defined in Title 18, United States Code, Section 2510(15). Internet users sign-up for a subscription for these electronic communication services by registering on the Internet with Rackspace. Rackspace requests subscribers to provide basic information, such as name, city/zip code, and other personal/biographical information, as well as payment information.
- b. Rackspace makes available to its users numerous services, to include, various operational resources for small business;
- c. Maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information;
- d. Subscribers to Rackspace may access their accounts on servers maintained or owned by Rackspace from any computer connected to the Internet located anywhere in the world;
  - i. Any email that is sent to a Rackspace subscriber is stored in the subscriber's "mail box" on Rackspace's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by the internet service

provider. If the message is not deleted by the subscriber, the account is below the storage limit, and the subscriber accesses the account periodically, that message can remain on Rackspace's servers indefinitely;

- ii. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Rackspace's servers, and then transmitted to its end destination. Rackspace users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Rackspace server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained at Rackspace, but that message will remain in the recipient's email box unless the recipient also deletes it or unless the recipient's account has exceeded its storage limitations;
- iii. A Rackspace subscriber can store files, including emails and image files, on servers maintained and/or owned by Rackspace; and,
- iv. Emails and image files stored on a Rackspace server by a subscriber may not necessarily also be located in the subscriber's home computer. The subscriber may store emails and/or other files on the Rackspace server for which there is insufficient storage space in the subscriber's own computer or

which the subscriber does not wish to maintain in his or her own computer. A search of the subscriber's home, business, or laptop computer will therefore not necessarily uncover files the subscriber has stored on the Rackspace servers.

#### **V. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

24. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Rackspace to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **VI. CONCLUSION**

25. Based on the foregoing, I believe there is probable cause to believe that the user(s) of the domain **polytainersinc.company.com** and the email accounts **bsattaur@polytainersinc.company.com**, **mjennings@polytainersinc.company.com**; **sachdeva@polytainersinc.company.com**; **kowalewski@polytainersinc.company.com**; and **jennings@polytainersinc.company.com** have committed violations of 18 U.S.C. § 1343; having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme, and that evidence of that

criminal violation, as specifically described in Attachment A to this application, is presently located at the subjects residence. There could also exist evidence of Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers) and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss) because unauthorized access to a computer is often used to acquire personal identifying information to carry out such schemes to defraud.

26. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe, that within the domain **polytainersinc.company.com** and the email accounts **bsattaur@polytainersinc.company.com**; **mjennings@polytainersinc.company.com**; **sachdeva@polytainersinc.company.com**; **kowalewski@polytainersinc.company.com**; and **jennings@polytainersinc.company.com** there exists evidence of violations of the and within the above-described accounts there exist evidence, contraband, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme); Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers) and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss). There is also probable cause to believe that this evidence is located on computer systems owned, maintained, and/or operated by **Rackspace US, Inc., 1 Fanatical Place, Windcrest, Texas 78218**. Therefore, I respectfully request that the Court issue a search warrant directed

to Rackspace for the email contents and other information described in Attachment A and following the search procedure described in Attachment B.

27. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

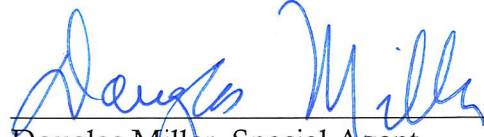
28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

## **VII. REQUEST FOR SEALING**

29. Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Disclosure of the search warrant at this time could jeopardize the investigation by giving the targets an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court



issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal for 60 days.

  
Douglas Miller, Special Agent  
Federal Bureau of Investigation

Sworn to before me this 19<sup>TH</sup> day of  
October, 2018.

  
JEREMIAH J. MCCARTHY  
United States Magistrate Judge

**ATTACHMENT A**  
**PROPERTY TO BE SEARCHED**

This warrant applies to information associated with the following accounts stored at the premises owned, maintained, controlled, or operated by Rackspace US, Inc., 1 Fanatical Place, Windcrest, Texas 78218.

**polytainersinc.company.com;**  
**bsattaur@polytainersinc.company.com;**  
**mjennings@polytainersinc.company.com;**  
**sachdeva@polytainersinc.company.com;**  
**kowalewski@polytainersinc.company.com;**  
**jennings@polytainersinc.company.com**

**ATTACHMENT B**

In order to ensure that agents search only those computer accounts and/or computer files described herein, this search warrant seeks authorization to permit employees of Rackspace, to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts and/or computer files described below, the following procedures have been implemented:

1. The warrant will be presented to Rackspace personnel by law enforcement agents. Rackspace personnel will be directed to isolate those accounts and files described below;
2. In order to minimize any disruption of computer service to innocent third parties, the system administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts and/or files described below;
3. The Rackspace system administrator will provide the exact duplicate of the accounts and files described below and all information stored in those accounts and /or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the system administrator and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;
5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the system administrator and will not further review the original duplicate absent an order of the Court.

**I. Information to be disclosed by Rackspace**

To the extent that the information described in Attachment A is within the possession, custody, or control of Rackspace, Rackspace is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails stored in the account, including copies of emails sent, email drafts, and deleted emails, if possible, from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, transactional log files containing logging activity, and means and source of payment (including any creditor bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All content in the Docs, Calendar, Friend Contacts and Photos areas;
- e. All records pertaining to communications between Rackspace, and any person regarding the account, including contacts with support services and records of actions taken.
- f. Any and all records pertaining to any payments for services provided by Rackspace to the account subscriber.

g. Any other domains and/or email accounts directly linked to the subject account via the domain **polytainersinc.company.com** and/or the email accounts within the **polytainersinc.company.com** domain, via cookie values, SMS, recovery, Android device, Apple device, other mobile device, secondary email, phone number, or other means. For all Rackspace accounts that are linked to any of the accounts listed in Attachment A by cookies, creation IP address, recovery email address, or telephone number, provide:

All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment(including any creditor bank account number)

h. Records pertaining to any Rackspace service provided that are linked to the domain **polytainersinc.company.com** and/or the email accounts within the **polytainersinc.company.com** domain.

## **II. Information to be searched for and seized by the government**

All records or information, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain

evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1343 (having devised a scheme to defraud, and to obtain money by means of false and fraudulent pretenses, representation, and promises, caused to be transmitted a wire communication in foreign commerce for the purpose of executing such scheme) and/or Title 18 U.S.C. §§ 1030(a)(4) (Fraud and Related Activity in Relation to Computers, and/or 1030(a)(5)(C) (Intentional Access to a Protected Computer Causing Damage or Loss), and/or, including, but not limited to, for each account or identifier listed on Attachment A, information pertaining to:

- a. The unauthorized access of email accounts;
- b. The contents of any such communications that will assist investigators in ascertaining the nature and scope of the crimes under investigation, the true identity and or location of the subjects and their co-conspirators, the names, addresses, and locations of victims; and any disposition of the proceeds of the crimes under investigation, including,
- c. Records relating to who created, used, or communicated with the account or identifier.
- d. For any and all accounts identified as being associated with targeted account through cookies, creation IP address, recovery email address, or telephone number, all subscriber records or information, not including contents. Records include but are not limited to records relating to who created, used, or communicated with the account or identifier.